Post-print of: Dougherty, ST and Fernández-Córdoba, C. “Kernels and ranks of cyclic and negacyclic quaternary codes” in Designs codes and cryptography (Springer), vol. 81 issue 2 (Nov. 2016) p. 347-364. The final versión is available at DOI 10.1007/s10623-015-0163-6

Kernels and Ranks of Cyclic and Negacyclic Quaternary Codes

Steven T. Dougherty
Department of Mathematics
University of Scranton
Scranton, PA 18510
USA
and
Cristina Fernández-Córdoba
Department of Information and Communications Engineering
Universitat Autònoma de Barcelona
08193-Bellaterra, Spain [*]

October 21, 2016

Abstract

We study the rank and kernel of $\mathbb{Z}_4$ cyclic codes of odd length n and give bounds on the size of the kernel and the rank. Given that a cyclic code of odd length is of the form $\mathcal{C} = \langle fh, 2fg \rangle$, where $fgh = x^n - 1$, we show that $\langle 2f \rangle \subseteq \mathcal{K}(\mathcal{C}) \subseteq \mathcal{C}$ and $\mathcal{C} \subseteq \mathcal{R}(\mathcal{C}) \subseteq \langle fh, 2g \rangle$ where $\mathcal{K}(\mathcal{C})$ is the preimage of the binary kernel and $\mathcal{R}(\mathcal{C})$ is the preimage of the space generated by the image of $\mathcal{C}$. Additionally, we show that both $\mathcal{K}(\mathcal{C})$ and $\mathcal{R}(\mathcal{C})$ are cyclic codes and determine $\mathcal{K}(\mathcal{C})$ and $\mathcal{R}(\mathcal{C})$ in numerous cases. We conclude by using these results to determine the case for negacyclic codes as well.

Key Words: Cyclic codes, quaternary codes, rank, kernel.
MSC: 94B15, 11T71

1 Introduction

A quaternary code of length n is a subset of $\mathbb{Z}_4^n$ and a binary code of length n is a subset of $\mathbb{F}_2^n$. For $\mathbb{Z}_4$ we say the code is linear if it is a module and for $\mathbb{F}_2$ we say it is linear if it is a vector space. Throughout this work, quaternary codes shall be denoted by calligraphic letters $\mathcal{C}, \mathcal{D}$ and binary codes will be denoted by standard type letters C, D.

[*]C. Fernández-Córdoba is with the Department of Information and Communications Engineering, Universitat Autònoma de Barcelona, 08193-Bellaterra, Spain (e-mail: cristina.fernandez@uab.cat), and with Barcelona Graduate School of Mathematics (BGSMath).

[†]This work has been partially supported by the Spanish MICINN grant TIN2013-40524-P and by the Catalan AGAUR grant 2014SGR-691.

Any linear $\mathbb{Z}_4$-code $\mathcal{C}$ is permutation-equivalent to a code with generator matrix of the form:

$$\begin{pmatrix} I_\delta & A & B \\ 0 & 2I_\gamma & 2C \end{pmatrix}, \tag{1}$$

where A and C are matrices over $\mathbb{F}_2$ and B is a matrix over $\mathbb{Z}_4$. It follows that $|\mathcal{C}| = 2^{2\delta+\gamma}$ and in this case we say that $\mathcal{C}$ is of type $4^\delta 2^\gamma$. This generator matrix is said to be in standard form. We say that a quaternary non-zero vector $\mathbf{v}$ is of order 2 if $\mathbf{v}+\mathbf{v} = \mathbf{0}$ and of order 4 if it is not of order 2 and $\mathbf{v}+\mathbf{v}+\mathbf{v}+\mathbf{v} = \mathbf{0}$.

The Hamming weight of any vector $\mathbf{u} \in \mathbb{F}_2^n$, denoted by $w_H(\mathbf{u})$, is the number of non-zero coordinates of $\mathbf{u}$. Given two binary vectors $\mathbf{u}, \mathbf{v} \in \mathbb{F}_2^n$, the Hamming distance between $\mathbf{u}$ and $\mathbf{v}$ is $d(\mathbf{u}, \mathbf{v}) = w_H(\mathbf{u}, \mathbf{v})$ and it is the number of coordinates in which they differ. The Lee weights of $0, 1, 2, 3 \in \mathbb{Z}_4$ are $0, 1, 2, 1$ respectively, and the Lee weight of $\mathbf{u} \in \mathbb{Z}_4^n$, $w_L(\mathbf{u})$, is the rational sum of the Lee weights of its components. If $\mathbf{u}, \mathbf{v} \in \mathbb{Z}_4^n$, then the Lee distance between $\mathbf{u}$ and $\mathbf{v}$ is $d_L(\mathbf{u}, \mathbf{v}) = w_L(\mathbf{u} - \mathbf{v})$.

Denote by ϕ the standard Gray map $\phi : \mathbb{Z}_4 \to \mathbb{F}_2^2$ that is defined by $0 \to 00, 1 \to 01, 2 \to 11, 3 \to 10$. We extend this map to $\mathbb{Z}_4^n \to \mathbb{F}_2^{2n}$ by applying it coordinatewise. The map is a non-linear distance preserving map. If $\mathcal{C} \subseteq \mathbb{Z}_4^n$ is a quaternary code with minimum distance d, then $\phi(\mathcal{C}) \subseteq \mathbb{F}_2^{2n}$ is a binary code with the same minimum distance. This map was used in [11] to show that certain non-linear binary codes had a $\mathbb{Z}_4$ structure.

We take the standard inner-product, namely $[\mathbf{v}, \mathbf{w}] = \sum v_i w_i$. For a linear code C over any alphabet, define its dual code as $C^\perp = \{\mathbf{w} \mid [\mathbf{w}, \mathbf{v}] = 0, \forall \mathbf{v} \in \mathcal{C}\}$. The code $C^\perp$ is a linear code whether or not C is.

We say that a code C over any alphabet is cyclic if

$$(c_0, c_1, \ldots, c_{n-1}) \in C \Rightarrow (c_{n-1}, c_0, c_1, \ldots, c_{n-2}) \in C$$

and that it is negacyclic if

$$(c_0, c_1, \ldots, c_{n-1}) \in C \Rightarrow (-c_{n-1}, c_0, c_1, \ldots, c_{n-2}) \in C.$$

We denote the cyclic shift by π, that is

$$\pi((c_0, c_1, \ldots, c_{n-1})) = (c_{n-1}, c_0, c_1, \ldots, c_{n-2})$$

and the negacyclic shift by σ, that is

$$\sigma((c_0, c_1, \ldots, c_{n-1})) = (-c_{n-1}, c_0, c_1, \ldots, c_{n-2}).$$

We say that C is quasi-cyclic of index k if $\pi^k(C) = C$ and k is the least integer satisfying this equation.

As usual we associate cyclic codes over a ring R with ideals in $R[x]/\langle x^n - 1\rangle$ and negacyclic codes with ideals in $R[x]/\langle x^n + 1\rangle$, where the vector $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1})$ corresponds to the polynomial $c(x) = c_0 + c_1 x + c_2 x^2 + \ldots + c_{n-1}x^{n-1}$. Throughout this paper, we will write c intead of $c(x)$ when we refer to the polynomial. Moreover, when we say that a quaternary code is cyclic we are assuming that the code is linear. However, when we say a binary code is quasi-cyclic we are not assuming that it is linear.

In [13], Pless and Qian describe cyclic codes over $\mathbb{Z}_4$ building on the earlier work of Calderbank and Sloane in [6] who studied cyclic codes over $\mathbb{Z}_{p^e}$ and the p-adic integers. The following fundamental theorem can be found in [13].

Theorem 1 *Let $\mathcal{C}$ be a $\mathbb{Z}_4$ cyclic code of odd length n. Then there are unique, monic polynomials f, g, and h such that $\mathcal{C} = \langle fh, 2fg \rangle$, where $fgh = x^n - 1$ and $|\mathcal{C}| = 4^{\deg(g)} 2^{\deg(h)}$.*

From the definition of the type of a quaternary cyclic code, if $\mathcal{C} = \langle fh, 2fg \rangle$ is a quaternary cyclic code of type $4^\delta 2^\gamma$, we have that $\delta = \deg(g)$ and $\gamma = \deg(h)$.

Recall that $(x^n - 1) = (x - 1)(x^{n-1} + x^{n-2} + \ldots + x + 1)$. This means that $x - 1$ and $x^{n-1} + x^{n-2} + \ldots + x + 1$ are always divisors of $x^n - 1$. For the remainder of the paper we assume that n is odd. This is because if n is odd there is a unique factorization of $x^n - 1$ into basic irreducible polynomials over the binary field. Then, using Hensel's lift, we have a unique factorization into basic irreducible pairwise coprime polynomials. Cyclic and negacyclic codes have also been studied for even lengths, see [1], [2], [3] and [8]. However, the description of the ideals is quite different for even lengths because the factorization of $x^n - 1$ is not unique in these cases.

For $u \in \mathbb{Z}_4[x]$, we denote by $\widetilde{u} \in \mathbb{F}_2[x]$ the polynomial obtained by considering the coefficients of u modulo 2. Note that if u is a divisor of $x^n - 1$ in $\mathbb{Z}_4[x]$, then $\widetilde{u}$ is a divisor of $x^n - 1$ in $\mathbb{F}_2[x]$. Let β be a primitive root of unity over $\mathbb{F}_2$ and $\widetilde{u}|(x^n - 1)$. We define $(\widetilde{u} \otimes \widetilde{u})|(x^n - 1)$ in $\mathbb{F}_2[x]$ as the polynomial whose roots are β^{i+j} such that β^i, β^j are roots of $\widetilde{u}$.

Let $\mathcal{C}$ be a $\mathbb{Z}_4$ cyclic code. The following theorem proved in [14] determines the linearity of $\phi(\mathcal{C})$ in terms of the generator polynomials of $\mathcal{C}$.

Theorem 2 *Let $\mathcal{C} = \langle fh, 2fg \rangle$ be a quaternary cyclic code, where $fgh = x^n - 1$. Let $\widetilde{e}$ be such that $x^n - 1 = (\widetilde{g} \otimes \widetilde{g})\widetilde{e}$ in $\mathbb{F}_2[x]$. The following properties are equivalent.*

1. *$\phi(\mathcal{C})$ is a binary linear code;*
2. *$(\widetilde{g} \otimes \widetilde{g})$ divides $\widetilde{h}\widetilde{g}$ in $\mathbb{F}_2[x]$;*
3. *$\widetilde{f}$ divides $\widetilde{e}$ in $\mathbb{F}_2[x]$.*

Corollary 1 *Let $\mathcal{C} = \langle fh, 2fg \rangle$ be a quaternary cyclic code, where $fgh = x^n - 1$.*

1. *If $f = 1$, then $\phi(\mathcal{C})$ is linear.*
2. *If $g = 1$, then $\phi(\mathcal{C})$ is linear.*
3. *If $g = x - 1$, then $\phi(\mathcal{C})$ is linear.*

Proof: If $f = 1$, then $\widetilde{f} = 1$ and $\phi(\mathcal{C})$ is linear by Theorem 2, item 3. If $g = 1$ or $g = x - 1$, then $(\widetilde{g} \otimes \widetilde{g}) = \widetilde{g}$ and $\phi(\mathcal{C})$ is linear by Theorem 2, item 2. □

We make the standard definition of the kernel of a binary code and introduce notation for its quaternary preimage.

If C is a binary code, define its kernel to be $ker(C) = \{\mathbf{v} \in C \mid \mathbf{v} + C = C\}$. If $\mathcal{C}$ is a quaternary code then its kernel is defined to be $\mathcal{K}(\mathcal{C}) = \{\mathbf{v} \in \mathcal{C} \mid \phi(\mathbf{v}) \in ker(\phi(\mathcal{C}))\}$.

It is well known that the kernel of a binary code is the intersection of all maximal linear subspaces and that the code is the union of cosets of the kernel; see [9], [10] for details.

Let C be a binary, not necessarily linear code. We denote by $\langle C \rangle$ the linear binary code generated by the vectors in C. We shall say that $rank(C) = dim(\langle C \rangle)$. For a quaternary code $\mathcal{C}$ we shall also say that $rank(\mathcal{C}) = rank(\phi(C))$.

We define the quaternary preimage of $\langle \phi(\mathcal{C}) \rangle$ as $\mathcal{R}(\mathcal{C})$, that is $\phi(\mathcal{R}(\mathcal{C})) = \langle \phi(\mathcal{C}) \rangle$. We have that $ker(\phi(\mathcal{C})) \subseteq \phi(\mathcal{C}) \subseteq \langle \phi(\mathcal{C}) \rangle$.

The following appears in [9].

Lemma 1 *Let $\mathcal{C}$ be a quaternary linear code. Then, $\mathcal{R}(\mathcal{C})$ and $\mathcal{K}(\mathcal{C})$ are quaternary linear codes satisfying*

$$\mathcal{K}(\mathcal{C}) \subseteq \mathcal{C} \subseteq \mathcal{R}(\mathcal{C}).$$

In [9], [10], various bounds are put on the rank and size of the kernel for arbitrary quaternary codes. In this work, these bounds are significantly refined for the cyclic case. Moreover, we show that, unlike the general case, it is not true that the intermediate dimensions for the rank and kernel between the bounds can be achieved for some code.

Both in the case of the rank and in the case of the dimension of the kernel, we will study subcodes of quaternary cyclic codes that are also quaternary cyclic. We will use the following theorem that relates the generator polynomials of a quaternary cyclic code and its quaternary cyclic subcodes.

Theorem 3 *Let $\mathcal{C}_0 = \langle fh, 2fg \rangle$, $\mathcal{C}_1 = \langle f'h', 2f'g' \rangle$ be quaternary cyclic codes of odd length with $\mathcal{C}_0 \subseteq \mathcal{C}_1$. Then f' divides f.*

Proof: If $y \in \mathcal{C}_1 = \langle f'h', 2f'g' \rangle$ then $y = f'h'j' + 2f'g'k'$ where j' and k' are polynomials. Then, $y = f'(h'j' + 2g'k')$. This gives that if $y \in \mathcal{C}_1$ then f' divides y.

Now $fh \in \mathcal{C}_0 \subseteq \mathcal{C}_1$ and $2fg \in \mathcal{C}_0 \subseteq \mathcal{C}_1$. This gives that f' divides fh and f' divides $2fg$. Then since h and g are coprime, then f' divides f. $\square$

2 Kernels of Cyclic Codes

In this section, we shall examine the kernel of quaternary cyclic codes.

For vectors $\mathbf{v}, \mathbf{w} \in \mathbb{Z}_4^n$, define $\mathbf{v} * \mathbf{w} = (v_1 w_1, v_2 w_2, \ldots, v_n w_n)$. The following is well known, see [11], and follows from the fact that $\phi(\mathbf{v}+\mathbf{w}) = \phi(\mathbf{v}) + \phi(\mathbf{w}) + \phi(2\mathbf{v} * \mathbf{w})$.

Lemma 2 *Let $\mathcal{C}$ be a quaternary linear code, $\mathbf{v} \in \mathcal{C}$. Then $\mathbf{v} \in \mathcal{K}(\mathcal{C})$ if and only if $2\mathbf{v} * \mathbf{w} \in \mathcal{C}$ for all $\mathbf{w} \in \mathcal{C}$.*

The following is immediate from the definitions.

Lemma 3 *Let $\mathcal{C}$ be a quaternary cyclic code of odd length n. Then $ker(\phi(\mathcal{C}))$ is a linear quasi-cyclic code of index 2 and $\phi(\mathcal{C})$ is a quasi-cyclic code of index 2 possibly non-linear.*

It is well known that $\phi(\mathcal{C})$ can be expressed as the union of cosets of $ker(\phi(\mathcal{C})$, specifically

$$\phi(\mathcal{C}) = \bigcup(\phi(\mathbf{v}_i) + ker(\phi(\mathcal{C}))),$$

where $\mathbf{v}_i$ is either $\mathbf{0}$ or any of the order 4 vectors in $\mathcal{C}$ that are not in $\mathcal{K}(\mathcal{C})$. That is, $\phi(\mathcal{C})$ is the union of cosets of the kernel. The coset leaders are precisely the images of those order 4 vectors which are not in the kernel. By the action of π^2, the quasi-cyclic shift sends coset to coset fixing only the kernel.

We already know that the kernel $\mathcal{K}(\mathcal{C})$ of any quaternary linear code is a quaternary linear code. The next theorem will show that $\mathcal{K}(\mathcal{C})$ is cyclic when $\mathcal{C}$ is cyclic.

Theorem 4 *Let $\mathcal{C}$ be a quaternary cyclic code. Then $\mathcal{K}(\mathcal{C})$ is a quaternary cyclic code.*

Proof: Let $\mathcal{C}$ be a quaternary cyclic code. Since $\mathcal{K}(\mathcal{C})$ is linear, we only have to check that $\pi(\mathbf{v}) \in \mathcal{K}(\mathcal{C})$, for $\mathbf{v} \in \mathcal{K}(\mathcal{C})$; that is, $2\pi(\mathbf{v}) * \mathbf{w} \in \mathcal{C}$, for all $\mathbf{w} \in \mathcal{C}$.

Let $\mathbf{v} \in \mathcal{K}(\mathcal{C}), \mathbf{w} \in \mathcal{C}$. We have that $2\pi(\mathbf{v}) * \mathbf{w} = \pi(2\mathbf{v} * \pi^{-1}(\mathbf{w}))$. Since $\mathbf{v} \in \mathcal{K}(\mathcal{C})$ and $\pi^{-1}(\mathbf{w}) \in \mathcal{C}$, $2\mathbf{v} * \pi^{-1}(\mathbf{w}) \in \mathcal{C}$ by Lemma 2. Moreover, since the code $\mathcal{C}$ is cyclic, $\pi(2\mathbf{v} * \pi^{-1}(\mathbf{w})) \in \mathcal{C}$, which gives that $2\pi(\mathbf{v}) * \mathbf{w} \in \mathcal{C}$, and $\pi(\mathbf{v}) \in \mathcal{K}(\mathcal{C})$. $\square$

Since $\mathcal{K}(\mathcal{C})$ is a quaternary cyclic code, we can write the kernel as $\mathcal{K}(\mathcal{C}) = \langle f'h', 2f'g' \rangle$ where $f'g'h' = x^n - 1$. Moreover, since $\mathcal{K}(\mathcal{C}) \subseteq \mathcal{C}$, if $\mathcal{C} = \langle fh, 2fg \rangle$, then f divides f' by Theorem 3.

The following theorem puts a minimal size on the kernel of the code. When the size of the kernel of a code is the minimal size, we say that the kernel is a minimum. First note that from Lemma 2 all order 2 codewords are in the kernel. In the case of a quaternary cyclic code $\mathcal{C} = \langle fh, 2fg \rangle$, the subgroup of order 2 codewords is $\langle 2fh, 2fg \rangle$. Moreover, since $gcd(h, g) = 1$, we have that $\langle 2fh, 2fg \rangle = \langle 2f \rangle$ and therefore, $\langle 2f \rangle \subseteq \mathcal{K}(\mathcal{C})$.

Theorem 5 *Let $\mathcal{C} = \langle fh, 2fg \rangle$ be a quaternary cyclic code of odd length. If $\mathcal{K}(\mathcal{C})$ is a minimum then $\mathcal{K}(\mathcal{C}) = \langle 2f \rangle$ and $|\mathcal{K}(\mathcal{C})| = 2^{n-\deg(f)}$. Hence the minimum size of $\mathcal{K}(\mathcal{C})$ is $2^{n-\deg(f)}$.*

Proof: Since $\langle 2f \rangle \subseteq \mathcal{K}(\mathcal{C}) = \langle f'h', 2f'g' \rangle$, the kernel of $\mathcal{C}$ is a minimum if $\mathcal{K}(\mathcal{C}) = \langle 2f \rangle$. Then invoke Theorem 1, with $g' = 1, f' = f$ and $h' = \frac{x^n-1}{f}$, and we have the result. $\square$

We can use this theorem to put a lower bound on the size of the kernel. The upper bound is reached when the code is linear, and we say that the kernel is a maximum. We can then establish an upper and a lower bound on the size of the kernel in the following corollary.

Corollary 2 *Let $\mathcal{C}$ be a quaternary cyclic code of odd length then*

$$2^{n-\deg(f)} \leq |\mathcal{K}(\mathcal{C})| \leq 4^{\deg(g)} 2^{\deg(h)}. \tag{2}$$

It follows that

$$\deg(g) + \deg(h) \leq dim(ker(\phi(\mathcal{C}))) \leq 2\deg(g) + \deg(h). \tag{3}$$

Proof: The lower bound follows from Theorem 5 and the upper bound follows from Theorem 1 given that $|\mathcal{C}| = 4^{\deg(g)}2^{\deg(h)}$. $\square$

Note that from [9], we know that if $\mathcal{C}$ is of type $4^\delta 2^\gamma$ then

$$\gamma + \delta \leq dim(ker(\phi(\mathcal{C}))) \leq \gamma + 2\delta.$$

Equation (3) simply rephrases this in terms of the degrees of the generating polynomials.

According to Theorem 1 and Theorem 5, the kernel of a quaternary cyclic code $\mathcal{C}$ is a minimum if $\mathcal{K}(\mathcal{C}) = \langle 2f \rangle$ and it is a maximum if $\phi(\mathcal{C})$ is linear and $\mathcal{K}(\mathcal{C}) = \mathcal{C}$. Of course, it is possible that the lower bound can equal the upper bound; for example, if $\mathcal{C} = \langle 2f \rangle$ then the kernel is both the maximum and the minimum. In this case we prefer to say that the kernel has maximum size, since maximum size indicates that the image is a linear binary code.

In the general linear case, we can find quaternary linear codes of length n and all possible values for the kernel as in the following theorem.

Theorem 6 ([9]) *There exists a quaternary linear code $\mathcal{C}$ of length n and type $4^\delta 2^\gamma$ with $ker(C) = \gamma + 2\delta - \bar{k}$ if and only if*

$$\begin{cases} \bar{k} \in \{0\} \cup \{2, \ldots, \delta\}, & \text{if} \quad s \geq 2, \\ \bar{k} \in \{0\} \cup \{2, \ldots, \delta\} \text{ and } \bar{k} \text{ even}, & \text{if} \quad s = 1, \\ \bar{k} = 0, & \text{if} \quad s = 0, \end{cases}$$

where $s = \beta - (\gamma - \kappa) - \delta$.

As it was mentioned in the introduction, this is not true for quaternary cyclic codes. We will establish some properties for the kernel of a quaternary cyclic code and we will give some conditions for its dimension. After that, we can begin to describe the kernel of a cyclic code in various cases.

We know that $\mathcal{K}(\mathcal{C}) = \langle f'h', 2f'g' \rangle$. The following theorem proves that, in fact, $\mathcal{K}(\mathcal{C}) = \langle fh', 2fg' \rangle$.

Theorem 7 *Let $\mathcal{C} = \langle fh, 2fg \rangle$ be a quaternary cyclic code of odd length with $\mathcal{K}(\mathcal{C}) = \langle f'h', 2f'g' \rangle$. Then $f' = f$.*

Proof: Since $\mathcal{K}(\mathcal{C}) \subseteq \mathcal{C}$, we have that $\langle f'h', 2f'g' \rangle \subseteq \langle fh, 2fg \rangle$. Then, by Theorem 3, f divides f'.

By the proof of Theorem 5, $\langle 2f \rangle \subseteq \langle f'h', 2'f'g' \rangle$. Since $\langle 2f \rangle = \langle x^n - 1, 2f \rangle = \langle f((x^n - 1)/f), 2f \rangle$, then by Theorem 3 we have that f' divides f. Hence $f' = f$. $\square$

As it was mentioned in the introduction, the kernel of a binary code is the intersection of all maximal linear subspaces. Therefore, if $\mathcal{C}_1$, $\mathcal{C}_2, \ldots \mathcal{C}_r$ are all the maximal subcodes of a quaternary linear code $\mathcal{C}$ such that $\phi(\mathcal{C}_i)$ is a linear subcode of $\phi(\mathcal{C})$, for $1 \leq i \leq r$, then

$$\mathcal{K}(\mathcal{C}) = \cap_{i=1}^{r} \mathcal{C}_i. \tag{4}$$

We will see in Proposition 1 the relation between the generator polynomials of the kernel and the generators polynomials of the maximal subcodes $\mathcal{C}_i$. First we need the following Lemma.

Lemma 4 *Let $\mathcal{C}_1 = \langle fh_1, 2fg_1\rangle$ and $\mathcal{C}_2 = \langle fh_2, 2fg_2\rangle$ be quaternary cyclic codes of odd length n. Then*

$$\mathcal{C}_1 \cap \mathcal{C}_2 = \langle f \operatorname{lcm}(h_1, h_2), 2f \gcd(g_1, g_2)\rangle.$$

Proof: First we will prove that $\langle f \operatorname{lcm}(h_1, h_2), 2f \gcd(g_1, g_2)\rangle \subseteq \mathcal{C}_1 \cap \mathcal{C}_2$. The generator $f \operatorname{lcm}(h_1, h_2) = fh_1 \frac{\operatorname{lcm}(h_1,h_2)}{h_1}$ that is in $\mathcal{C}_1$. Since $gcd(h_1, g_1) = 1$, there exist $\lambda, \mu \in \mathbb{Z}_4[x]$ such that $2f\gcd(g_1, g_2) = 2fgcd(g_1, g_2)(g_1\lambda + h_1\mu)$ that belongs to $\mathcal{C}_1$. Therefore $\langle f \operatorname{lcm}(h_1, h_2), 2f \gcd(g_1, g_2)\rangle \subseteq \mathcal{C}_1$. Using the same argument for $\mathcal{C}_2$ we obtain the inclusion.

Finally, we will prove the other inclusion. Since $\mathcal{C}_1 \subseteq \mathcal{C}_1 \cap \mathcal{C}_2$, we have by Therorem 3 that $\mathcal{C}_1 \cap \mathcal{C}_2 = \langle fh', 2fg'\rangle$. Since fh_1 and fh_2 divides h', we have that $f \operatorname{lcm}(h_1, h_2) | fh$. Therefore $\langle fh', 2fg'\rangle \subseteq \langle f \operatorname{lcm}(h_1, h_2), 2\frac{x^n-1}{\operatorname{lcm}(h_1,h_2)}\rangle$. Since $fh_1g_1 = fh_2g_2 = x^n - 1$, it is easy to check that $\operatorname{lcm}(h_1, h_2) \cdot \gcd(g_1, g_2) = \frac{x^n-1}{f} = h_1g_1 = h_2g_2$. Hence, $\frac{x^n-1}{\operatorname{lcm}(h_1,h_2)} = 2f \gcd(g_1, g_2)$ and the results follows. □

Proposition 1 *Let $\mathcal{C} = \langle fh, 2fg\rangle$ be a quaternary cyclic code of odd length. Let $\mathcal{C}_1$, $\mathcal{C}_2, \ldots \mathcal{C}_r$ be all the maximal subcodes of a $\mathcal{C}$ such that $\phi(\mathcal{C}_i)$ is a linear subcode of $\phi(\mathcal{C})$. Therefore*

1. *$\mathcal{C}_i = \langle fh_i, 2fg_i\rangle$, for $i \in \{1, \ldots, r\}$.*
2. *$\mathcal{K}(\mathcal{C}) = \langle fh', 2fg'\rangle$, where $h' = \operatorname{lcm}(h_1 \ldots, h_r)$ and $g' = \gcd(g_1, \ldots, g_r)$.*

Proof: For $i \in \{1, \ldots, r\}$, $\mathcal{C}_i$ is quaternary cyclic code. Hence, $\mathcal{C}_i = \langle f_ih_i, 2f_ig_i\rangle$. We have that $\langle 2f\rangle \subseteq \mathcal{K}(\mathcal{C}) \subseteq \langle fh, 2fg\rangle$. Then, by aplying the same argument as in the proof of Theorem 7, we have that $f_i = f$.

Item 2 is obteined by extending Lemma 4 to $\mathcal{C}_1 \cap \cdots \cap \mathcal{C}_r$. □

Let $\mathbf{1}$ denote the all-one vector. Note that $\mathbf{1}$ corresponds to the polynomial $x^{n-1} + x^{n-2} + \ldots + x + 1$. The following lemma was proven in a different way in [5].

Lemma 5 *Let $\mathcal{C}$ be a quaternary code. If $\mathbf{1} \in \mathcal{C}$ then $\mathbf{1} \in \mathcal{K}(\mathcal{C})$.*

Proof: We have that $2 \cdot \mathbf{1} * \mathbf{v} = 2\mathbf{v} \in \mathcal{C}$ for all vectors $\mathbf{v}$ in $\mathcal{C}$. By Lemma 2, this gives that if the all-one vector is in the code $\mathcal{C}$ then it is in the kernel $\mathcal{K}(\mathcal{C})$. □

Note that the proof of this lemma applies to any vector over $\mathbb{Z}_4$ that consists entirely of units.

Since we have that $\langle 2f\rangle \in \mathcal{K}(\mathcal{C})$, if $\mathbf{1} \in \mathcal{K}(\mathcal{C})$, then we have that the size of the kernel is not a minimum; that is $dim(ker(\phi(C))) \geq \gamma + \delta + 1$.

With the following theorem and corollary we shall see when the size is exactly $\gamma + \delta + 1$.

Theorem 8 *Let $\mathcal{C} = \langle fh, 2fg\rangle$ be a quaternary cyclic code of odd length n. If $\mathbf{v} \in \mathcal{K}(\mathcal{C})$ is an order 4 vector, then $dim(ker(\phi(\mathcal{C})) \geq \deg(g) + \deg(h) + n - \deg(v)$, where v is the polynomial corresponding to $\mathbf{v}$.*

Proof: First we note that $\deg(g) + \deg(h)$ is the minimum dimension of the kernel, and all order 2 codewords are in the kernel by Theorem 5. If $\mathbf{v} \in \mathcal{K}(\mathcal{C})$ then all n cyclic shifts of $\mathbf{v}$ are in $\mathcal{K}(\mathcal{C})$ since $\mathcal{K}(\mathcal{C})$ is a cyclic code. But $n - \deg(v)$ cyclic shifts are linearly independent over $\mathbb{Z}_4$, adding $n - \deg(v)$ to the dimension of the binary kernel (noting that the order 2 codewords were already in $\mathcal{K}(\mathcal{C})$). $\square$

Corollary 3 *Let $\mathcal{C} = \langle fh, 2fg \rangle$ be a quaternary cyclic code of odd length. If $dim(\phi(\mathcal{C})) = \deg(g) + \deg(h) + 1$, then $\mathcal{K}(\mathcal{C}) = \langle x^{n-1} + x^{n-2} + \ldots + x + 1, 2f(x-1) \rangle$.*

Proof: Since the minimal kernel contains all order 2 codewords, to increase the dimension by one a unique order 4 vector $\mathbf{v}$ must be added. By Theorem 8, this vector must increase the dimension by $n - \deg(v)$ where v is the polynomial corresponding to the vector $\mathbf{v}$. However, the only polynomial divisor of $x^n - 1$ with degree $n - 1$ is the polynomial $x^{n-1} + x^{n-2} + \ldots + x + 1$. $\square$

Finally, the possible values on the size of the kernel depends on the degree of the polynomials dividing g.

Theorem 9 *Let $\mathcal{C} = \langle fh, 2fg \rangle$ be a quaternary cyclic code of odd length. Then, there exists k dividing g such that $\mathcal{K}(\mathcal{C}) = \langle fhk, 2f\frac{g}{k} \rangle$.*

Proof: From Theorem 7, we have that $\mathcal{K}(\mathcal{C}) = \langle fh', 2fg' \rangle$, for some g', h' such that $x^n - 1 = fh'g'$. Since $fh' \in \mathcal{C}$, we have that $fh' = af h + b2fg$, and hence $h' = ah + b2g$, for some $a, b \in \mathbb{Z}_4[x]$. In $\mathbb{F}_2[x]$, we have $\widetilde{h'} = \widetilde{a}\widetilde{h}$, with $\widetilde{h'}$ and $\widetilde{h}$ dividing $x^n - 1$ in $\mathbb{F}_2[x]$. Let k be the Hensel lift of $\widetilde{a}$ in $\mathbb{Z}_4[x]$. Then we have $h' = kh$.

Finally, since $x^n - 1 = fgh = fg'h' = fg'hk$, we have that $g'k = g$ and hence $\mathcal{K}(\mathcal{C}) = \langle fhk, 2f\frac{g}{k} \rangle$ with k dividing g. $\square$

Corollary 4 *Let $\mathcal{C} = \langle fh, 2fg \rangle$ be a quaternary cyclic code of odd length. Hence, $dim(ker(\phi(\mathcal{C})) = 2\deg(g) + \deg(h) - \deg(k)$, where k is a polynomial dividing g.*

Proof: From Theorem 9, $\mathcal{K}(\mathcal{C}) = \langle fhk, 2f\frac{g}{k} \rangle$. Let $g' = \frac{g}{k}$. Then, $dim(ker(\phi(\mathcal{C})) = 2\deg(g') + \deg(hk) = 2\deg(g) - 2\deg(k) + \deg(h) + \deg(k) = 2\deg(g) + \deg(h) - \deg(k)$. $\square$

But not all the possible kernels are realized as shown in the following theorem.

Theorem 10 *Let $\mathcal{C} = \langle fh, 2fg \rangle$ be a quaternary cyclic code of odd length with kernel $\mathcal{K}(\mathcal{C}) = \langle fh', 2fg' \rangle$. If $(x-1)$ divides g then $(x-1)$ also divides g'.*

Proof: Let $\mathcal{C} = \langle fh, 2fg \rangle$, with $(x-1)$ dividing g and $k(\mathcal{C}) = \langle fh', 2fg' \rangle$. Consider the maximal subcodes $\mathcal{C}_1, \ldots, \mathcal{C}_r$ as in Equation (4). We have that $\mathcal{K}(\mathcal{C}) = \cap_{i=0}^{r} \mathcal{C}_i$, and $\phi(\mathcal{C}_i)$ is linear.

Suppose $(x-1)$ does not divide g'. By Proposition 1, $\{\mathcal{C}_i = \langle fh_i, 2fg_i \rangle\}_{1 \le i \le r}$, and there exists $j \in \{1, \ldots, r\}$ such that g does not divide g_j. We have that

$(\widetilde{g_j} \otimes \widetilde{g_j})$ divides $\widetilde{h_j}\widetilde{g_j}$ by Theorem 2. Consider $g^\bullet = g_j(x-1)$ and $h^\bullet = \frac{h_j}{(x-1)}$. It is easy to check that $(\widetilde{g^\bullet} \otimes \widetilde{g^\bullet}) = \mathrm{lcm}((\widetilde{g_j} \otimes \widetilde{g_j})(x-1), g_j)$ which divides $h_j g_j$. Since $g^\bullet h^\bullet = g_j h_j$, we have that $(\widetilde{g^\bullet} \otimes \widetilde{g^\bullet})$ divides $\widetilde{h^\bullet}\widetilde{g^\bullet}$ and, by Therorem 2, the image under the Gray map of the code $\mathcal{C}^\bullet = \langle fh^\bullet, 2fg^\bullet \rangle$ is linear. Finally, $\mathcal{C}_j \subset \mathcal{C}^\bullet \subseteq \mathcal{C}$ with $\phi(C^\bullet)$ linear, which is a contradiction with the fact that $\mathcal{C}_j$ is a maximal subcode with linear image under the Gray map.

□

Example 1 *Consider the case when $\mathcal{C} = \langle fh, 2fg \rangle$, with $g = (x-1)a$, where a is an irreducible polynomial. From Corollary 4, the dimension of the kernel, $\mathcal{K}(\mathcal{C}) = \langle fh', 2fg' \rangle$, is $2\deg(g) + \deg(h) - \deg(k)$, where $g'k = g$. Hence, the possible dimensions for the kernel are $\deg(g) + \deg(h), \deg(g) + \deg(h) + 1, 2\deg(g) + \deg(h) - 1$, and $2\deg(g) + \deg(h)$. But by Theorem 10, we have that $(x-1)$ does not divide k. Hence, $k = a$ or $k = 1$, and $\deg(k)$ is $\deg(g) - 1$ or 0. Then $\deg(g) + \deg(h)$ and $2\deg(g) + \deg(h) - 1$ are not possible dimensions.*

The next corollary describes the situation when $(x-1)$ divides g, but may not be equal to g.

Corollary 5 *Let $\mathcal{C} = \langle fh, 2fg \rangle$ be a quaternary cyclic code of odd length. If $(x-1)$ divides g then $\mathbf{1} \in \mathcal{K}(\mathcal{C})$ and so $\mathcal{K}(\mathcal{C})$ is not the minimum.*

Proof: If $(x-1)$ divides g then fh divides $x^{n-1} + x^{n-2} + \ldots + x + 1$. Hence the all-one vector is in the code and therefore $\mathbf{1} \in \mathcal{K}(\mathcal{C})$ by Lemma 5. But $\mathbf{1}$ is not in $\langle 2fh, 2fg \rangle$ since it is an order 4 vector and therefore $\mathcal{K}(\mathcal{C})$ is not the minimum. □

Theorem 11 *Let $\mathcal{C} = \langle fh, 2fg \rangle$ be a quaternary cyclic code of odd length. If $h = 1$ and $f \in \mathcal{K}(\mathcal{C})$ then $\mathcal{K}(\mathcal{C}) = \mathcal{C}$ and $\phi(\mathcal{C})$ is linear.*

Proof: If $h = 1$ then $fg = x^n - 1$ so $\mathcal{C} = \langle f \rangle$. If $f \in \mathcal{K}(\mathcal{C})$ then as in Theorem 4 all cyclic shifts of f are in $\mathcal{K}(\mathcal{C})$ and so $\mathcal{K}(\mathcal{C}) = \mathcal{C}$. □

As an example, let $n = 3$, then $x^3 - 1 = (x-1)(x^2 + x + 1)$. If $f = x^2 + x + 1$, $g = x - 1$ and $h = 1$, then $\mathcal{C} = \langle x^2 + x + 1 \rangle$ is generated by the all-one vector and this vector is in the kernel by Lemma 5, so $\mathcal{C} = \mathcal{K}(\mathcal{C})$ and $\phi(\mathcal{C})$ is linear.

It is not true that if f is not in the kernel then the kernel is a minimum. For example, consider $n = 9$ and $x^9 - 1 = (x-1)(x^2 + x + 1)(x^6 + x^3 + 1)$. If we take $f = x^6 + x^3 + 1$, $h = 1$, and $g = x^3 - 1$ then $\mathcal{C} = \langle x^6 + x^3 + 1 \rangle$ and the kernel does not contain $f = x^6 + x^3 + 1$ but does contains the all-one vector. Hence the kernel is not a minimum by Lemma 5. In fact, in this case the dimension of $ker(\phi(\mathcal{C}))$ is the minimum plus 1.

Theorem 12 *Let $\mathcal{C} = \langle fh, 2fg \rangle$ be a quaternary cyclic code of odd length with $\{f, g, h\} = \{1, x-1, x^{n-1} + x^{n-2} + \ldots + x + 1\}$. If $g = x^{n-1} + x^{n-2} + \ldots + x + 1$ and $h = 1$ then $\mathcal{K}(\mathcal{C}) = \langle 2(x-1) \rangle$, which is the minimum. In all other cases $\mathcal{K}(\mathcal{C}) = \mathcal{C}$ and the image is linear.*

Proof: If g is not the polynomial $x^{n-1}+x^{n-2}+\ldots+x+1$, then $g=1$ or $g=x-1$, and by Corollary 1 we have that $\mathcal{K}(\mathcal{C})=\mathcal{C}$. In these cases the code is either $\langle x^{n-1}+x^{n-2}+\ldots+x+1\rangle$, $\langle 2(x-1)\rangle$ or $\langle 2(x^{n-1}+x^{n-2}+\ldots+x+1)\rangle$.

Let $g=(x^{n-1}+x^{n-2}+\ldots+x+1)$. We have that $h=1$ or $h=x-1$. If $h=x-1$, then $f=1$ and therefore $\mathcal{K}(C)=C$ by Corollary 1.

If $h=1$, we have that $\mathcal{C}=\langle x-1\rangle$. Then the generator matrix of the code in standard form is:

$$\begin{pmatrix} 1 & 0 & 0 & \ldots & 0 & 3 \\ 0 & 1 & 0 & \ldots & 0 & 3 \\ \vdots & & & & & \\ 0 & 0 & 0 & \ldots & 1 & 3 \end{pmatrix}.$$

Let $\mathbf{v}_i$ be the i-th row of the matrix.

Then using Lemma 2, for arbitrary rows of this matrix $\mathbf{v}_i, \mathbf{v}_j$ we have $2\mathbf{v}_i * \mathbf{v}_j = (0,0,\ldots,0,2)$ which is not in $\mathcal{C}$. Let $\mathbf{u}$ be an order 4 vector. We can write $\mathbf{u}=\mathbf{u}'+2\bar{\mathbf{u}}$, where $\mathbf{u}'=\sum_{i\in A}\alpha_i\mathbf{v}_i$, $\alpha_i\in\{1,3\}$, $A\subseteq\{1,\ldots,n-1\}$. We have that $\mathbf{u}\in\mathcal{K}(\mathcal{C})$ if and only if $\mathbf{u}'\in\mathcal{K}(\mathcal{C})$. If there exists $j\in\{1,\ldots,n-1\}\setminus A$, then $2\mathbf{u}*\mathbf{v}_j=(0,0,\ldots,0,2)$ which is not in $\mathcal{C}$. If, on the other hand, there is no j which is not in A then $2\mathbf{u}=(2,2,2,\ldots,2,0)$. Hence, $2\mathbf{u}*\mathbf{v}_1=(2,0,0,\ldots,0)$ which is not in $\mathcal{C}$. Then there is no order 4 vector in the kernel. Therefore, $\mathcal{K}(\mathcal{C})=\langle 2(x-1)\rangle$ and the kernel is a minimum. □

3 Classification of the Kernels for Some Factorizations of x^n-1

In this section, we will take into account the factorization of x^n-1. Specifically, we shall examine the following cases. The first case is when the polynomial $x^{n-1}+x^{n-2}+\ldots+x+1$ is irreducible; that is, there are just two factors in the factorization of x^n-1. Then, we look at the case when there are three factors and in particular when this occurs for length $n=p^2$, where p a prime.

If the polynomial $x^{n-1}+x^{n-2}+\ldots+x+1$ is irreducible then the factorization of x^n-1 is

$$x^n-1=(x^{n-1}+x^{n-2}+\ldots+x+1)(x-1)$$

and there are $3^2=9$ possible codes. Applying Theorem 12 to this case we get the following corollary which determines the dimension of the kernel for all nine codes.

Corollary 6 *Let $\mathcal{C}=\langle fh, 2fg\rangle$ be a quaternary cyclic code of odd length. If $x^{n-1}+x^{n-2}+\ldots+x+1$ is irreducible over $\mathbb{Z}_4$, then if $g=x^{n-1}+x^{n-2}+\ldots+x+1$, $f=x-1$ and $h=1$ the kernel is a minimum and in all other cases $\mathcal{K}(\mathcal{C})=\mathcal{C}$ and the image is linear.*

Therefore, if $x^{n-1}+x^{n-2}+\ldots+x+1$ is irreducible, the only possible dimensions of the kernel are the minimum, $\gamma+\delta$, or the maximum $\gamma+2\delta$.

For example, for $n\leq 30$, the polynomial $x^{n-1}+x^{n-2}+\ldots+x+1$ is irreducible for $n=3,5,11,13,19,29$. Hence for these values of n, when $g=x^{n-1}+x^{n-2}+\ldots+x+1$ and $h=1$, the kernel is a minimum, and in all other cases we have that the image is a linear code.

Let $n = pq$, p, q integers. Then $(1 + x^p + x^{2p} + \ldots + x^{(q-1)p})(x^p - 1) = x^{qp} - 1 = x^n - 1$. Hence these two polynomials divide $x^n - 1$. We shall examine the case when fh is the first polynomial. Notice that $x^p - 1$ has further factors. These cases shall be examined later.

Theorem 13 *Let $\mathcal{C} = \langle fh, 2fg \rangle$ be a quaternary cyclic code of odd length. Let $n = pq$, p, q integers. If $fh = (1 + x^p + x^{2p} + \ldots + x^{(q-1)p})$ then $\mathcal{K}(\mathcal{C}) = \mathcal{C}$.*

Proof: The matrix given by taking p cyclic shifts of the fh, i.e. $\pi^i(fh)$ for $i = 0, 1, 2, \ldots, p-1$, is in standard form. That is, the identity matrix is in the first p coordinates. These are the vectors of order 4 in the generator matrix of the code. The generator matrix in the standard form also has other order 2 vectors which are not relevant to this proof. Then if we take $2\mathbf{v} * \mathbf{w}$ for any of these vectors we have $\mathbf{0}$ or $2\mathbf{v}$ which are in the code. Hence, the code $\mathcal{C}$ satisfies $\mathcal{K}(\mathcal{C}) = \mathcal{C}$. $\square$

We now consider the further factorization of $x^p - 1$.

Theorem 14 *Let $\mathcal{C} = \langle fh, 2fg \rangle$ be a quaternary cyclic code of odd length. If for some integer s we have that s divides n and $fh = x^{s-1} + \ldots + x + 1$, then $dim(ker(\phi(C))) \geq \gamma + \delta + 1$, that is, the kernel is not a minimum.*

Proof: We have seen above that $(1 + x^p + x^{2p} + \ldots + x^{(q-1)p})(x^p - 1) = x^{qp} - 1 = x^n - 1$ when $n = pq$, p, q integers. Let $p = s + 1$ then $x^s - 1 = (x - 1)(x^{s-1} + \ldots + x + 1)$ so this polynomial divides $x^n - 1$ when s divides n. Let $\mathbf{v}$ be the vector given by fh. Then

$$\mathbf{v} + \pi^s(\mathbf{v}) + \pi^{2s}(\mathbf{v}) + \ldots + \pi^{(q-1)(s)}(\mathbf{v}) = \mathbf{1}.$$

This gives that $\mathbf{1} \in \mathcal{C}$ and $\mathbf{1} \in \mathcal{K}(\mathcal{C})$ by Lemma 5. This gives the result. $\square$

Example 2 *Consider $n = 9$ and $s = 3$. Let $f = x^2 + x + 1$, $g = x^7 + 3x^6 + x^4 + 3x^3 + x + 3$ and $h = 1$. Then $dim(ker(\phi(\mathcal{C})) = \gamma + \delta + 1$. If $n = 15$ then letting $h = 1$ and $f = x^2 + x + 1$ or $f = x^4 + x^3 + x^2 + x + 1$ results in codes with $dim(ker(\phi(\mathcal{C})) = \gamma + \delta + 1$.*

Theorem 15 *If there are exactly three monic irreducible factors of $x^n - 1$, n odd, then $n = p$ or $n = p^2$ where $p > 2$ is a prime. If there are exactly two monic irreducible factors of $x^n - 1$ then $n = p$.*

Proof: If $n = st$ with $s \neq t$ then $x - 1, x + x^s + x^{2s} + \ldots + x^{(t-1)s}, x + x^t + x^{2t} + \ldots + x^{(s-1)t}, 1 + x + x^2 + \ldots + x^s$, and $1 + x + x^2 + \ldots + x^t$ are all distinct factors of $x^n - 1$ as we have shown previously. Hence the only time you can have three factors is when $n = p$ or $n = p^2$, where p is a prime. If $n = p^2$, then $x - 1, x + x^p + x^{2p} + \ldots + x^{(p-1)p}$ and $1 + x + x^2 + \ldots + x^p$ are factors, hence if there are only two factors then n is a prime. $\square$

We have seen in Theorem 15 that if we have three factors in the decomposition of $x^n - 1$ then $n = p$ or p^2. We will see some properties for these cases in general and we will give the complete classification for the case $n = p^2$.

Theorem 16 *Let $x^n-1=(x-1)ab$, where a and b are irreducible polynomials. Let $\mathcal{C}$ be a quaternary cyclic code of odd length with $\mathcal{C}=\langle a,(x-1)ab\rangle=\langle a\rangle$. Then either $\mathcal{K}(\mathcal{C})=\mathcal{C}$ and $\phi(\mathcal{C})$ is linear, or $dim(\phi(\mathcal{C}))=\gamma+\delta+1$.*

Proof: Writing $\mathcal{C}=\langle a\rangle$ in the form $\mathcal{C}=\langle fh,2fg\rangle$, we have $f=a$, $g=(x-1)b$, $h=1$. Then write $\mathcal{K}(\mathcal{C})=\langle fh',2fg'\rangle$ by Theorem 7. Since a divides $x^{n-1}+x^{n-2}+\ldots+x+1$, we have that $x^{n-1}+x^{n-2}+\ldots+x+1$ is in $\mathcal{K}(\mathcal{C})$, that is $\mathbf{1}\in\mathcal{K}(C)$. This gives that fh' must divide $x^{n-1}+x^{n-2}+\ldots+x+1$. The only possibilities are $fh'=1+x+x^2+\ldots+x^{n-1}$ or $fh'=f$ since f must divide fh' as the kernel is a subspace. If $fh'=f$ then $\mathcal{K}(\mathcal{C})=\mathcal{C}$. If $fh'=1+x+x^2+\ldots+x^{n-1}$ then $\mathcal{K}(\mathcal{C})=\langle 1+x+x^2+\ldots+x^{n-1},2f\rangle$ and $dim(\phi(ker(\mathcal{C}))$ is $\gamma+\delta+1$. $\square$

Let $x^n-1=(x-1)ab$, where a and b are irreducible polynomials. If $n=p^2$, p prime, then we can take $a=1+x+\cdots+x^{p-1}$ and $b=1+x^p+\cdots+x^{(p-1)p}$. However, when $n=p$ we do not have the same divisors of x^n-1. For example, we have $x^7-1=(x-1)(3+x+2x^2+x^3)(3+2x+3x^2+x^3)$ and $x^{17}-1=(x-1)(x^8+2x^6+3x^5+x^4+3x^3+2x^2+1)(x^8+x^7+3x^6+3x^4+3x^2+x+1)$.

Remark: If $n=p^2$, p prime, and $x^n-1=(x-1)ab$ with $a=1+x+\cdots+x^{p-1}$ and $b=1+x^p+\cdots+x^{(p-1)p}$, then the only self-dual $\mathbb{Z}_4$-cyclic code of length n is $\mathcal{C}=\langle 2\rangle$. This is because the code $\mathcal{C}$ is self-dual if and only if $\langle fh+2f\rangle=\langle g^*h^*+2g^*\rangle$ (see [12]); that is, $h=\pm h^*$ and $f=\pm g^*$, where h^* and g^* are the reciprocal polynomials of h and g respectively. Hence, the only option is $h=x^n-1$, $f=g=1$. This is not true if $n=p$. In the case $n=7$, for example, we have that $x^7-1=(x-1)(3+x+2x^2+x^3)(3+2x+3x^2+x^3)$ and the $\mathbb{Z}_4$-cyclic codes $\mathcal{C}_1=\langle(x-1)a,2ab\rangle$ and $\mathcal{C}_2=\langle(x-1)b,2ba\rangle$ are both self-dual, for $a=(3+2x+3x^2+x^3)$ and $b=(3+x+2x^2+x^3)$ since $a=-b^*$. Moreover, $\mathcal{C}_1$ and $\mathcal{C}_2$ are equivalent and, therefore the dimensions of the kernels coincide.

From now on, we will consider the case $n=p^2$ odd, $p>2$ prime and $(x-1)^n=(x-1)ab$, for $a=1+x+x^2+\ldots+x^{p-1}$ and $b=1+x^p+x^{2p}+\ldots+x^{(p-1)p}$. We will completely determine the kernel in this case for all possible values of f,g and h.

Theorem 17 *Let $\mathcal{C}=\langle fh,2fg\rangle$ be a quaternary cyclic code of odd length $n=p^2$ and $x^n-1=(x-1)ab$ where a and b are irreducible polynomials. Set $h=1$. If $f=a$, then $\mathcal{K}(\mathcal{C})=\langle 1+x+\cdots+x^{n-1},2ab\rangle$ and if $f=b$ then $\mathcal{K}(\mathcal{C})=\mathcal{C}$.*

Proof: Let $\mathcal{C}=\langle fh,2fg\rangle$ and $\mathcal{K}(\mathcal{C})=\langle fh',2fg'\rangle$, by Theorem 7, where fh divides fh'.

Consider $h=1$ and $f=a$. Then $\mathcal{C}=\langle a,2(1+x+\cdots+x^{n-1})\rangle$. Note that $2a\star\pi(a)\notin\mathcal{C}$ and hence $a\notin\mathcal{K}(\mathcal{C})$ and $\mathcal{K}(\mathcal{C})\neq\mathcal{C}$. Moreover, $1+x+\cdots+x^{n-1}=a+\pi^p(a)+\cdots+\pi^{p-1}(a)=\in\mathcal{C}$. Hence, by Lemma 5, $1+x+\cdots+x^{n-1}\in\mathcal{K}(\mathcal{C})$. Since $a=fh$ divides fh' and fh' divides $1+x+\cdots+x^{n-1}=ab$, we have that $h'=1$ or $h'=b$. If $h'=1$, then $\mathcal{K}(\mathcal{C})=\mathcal{C}$ that is not possible. Therefore, $h'=b$ and $\mathcal{K}(\mathcal{C})=\langle 1+x+\cdots+x^{n-1},2ab\rangle$.

Now consider $h=1$ and $f=b$. Then $\mathcal{C}=\langle b,2(1+x+\cdots+x^{n-1})\rangle$. Note that for all i, $2b\star\pi^i(b)$ is either 0 or $2b$ and, in both cases, it belongs to $\mathcal{C}$. Hence $b\in\mathcal{K}(\mathcal{C})$ and $\mathcal{K}(\mathcal{C})=\mathcal{C}$. $\square$

Theorem 18 *Let $\mathcal{C} = \langle fh, 2fg \rangle$ be a quaternary cyclic code of odd length $n = p^2$ and $x^n - 1 = (x-1)ab$ where a and b are irreducible polynomials. Set $h = 1$ and $g = a$ or $g = b$. Then $\mathcal{K}(\mathcal{C}) = \langle 2f \rangle$.*

Proof: Let $\mathcal{C} = \langle fh, 2fg \rangle$ and $\mathcal{K}(\mathcal{C}) = \langle fh', 2fg' \rangle$, by Theorem 7, where f divides fh'. Hence, $h' = 1$ and $\mathcal{K}(C) = \mathcal{C}$ or $h' = g$ and $\mathcal{K}(\mathcal{C}) = \langle 2f \rangle$. That is, if there is a codeword not in the kernel, we have that the kernel is a minimum.

First, consider $g = b$ and $f = (x-1)a = x^p - 1$. Let $\mathbf{v}$ be the vector corresponding to $x^p - 1$. Since $p > 2$, we have that $2\mathbf{v} \star \pi^p(\mathbf{v}) = \pi^p(2, 0, \ldots, 0)$ that belongs to $\mathcal{C}$ if and only if $(1, 0, \ldots, 0)$ belongs to $\mathcal{C}$, due to the fact that $\mathcal{C}$ is free, where a free code is a code isomorphic to $\mathbb{Z}_4^k$ for some k. In this case, we have that $1 + x + \cdots + x^{n-1}$ is in $\mathcal{C}$ that is not possible. Hence, $\pi^p(2, 0, \ldots, 0)$ is not in the code and $\mathcal{K}(\mathcal{C}) \neq \mathcal{C}$. Therefore, the kernel is a minimum.

Finally, consider $g = a$ and $f = (x-1)b$. Take the vector $\mathbf{v} = (130\ldots0\ 130\ldots0\ \ldots130\ldots0)$ corresponding to $(x-1)b$. The code is free and it is generated by $p-1$ independent vectors of order 4. A generator matrix of the code is

$$G = \begin{pmatrix} \mathbf{v} \\ \pi(\mathbf{v}) \\ \vdots \\ \pi^{p-2}(\mathbf{v}) \end{pmatrix} = \begin{pmatrix} 130\ldots0130\ldots0\cdots130\ldots0 \\ 013\ldots0013\ldots0\cdots013\ldots0 \\ \ddots \\ 0\ldots0130\ldots013\cdots0\ldots013 \end{pmatrix}$$

Note that $2\mathbf{v} \star \pi(\mathbf{v}) = (020\ldots020\ldots0\ldots020\ldots0)$ and it is in the code if and only if $(010\ldots010\ldots0\ldots010\ldots0)$ also belongs to the code which is not true by the form of the generator matrix. Hence, $2\mathbf{v} \star \pi(\mathbf{v}) \notin \mathcal{C}$ and $\mathbf{v}$ is not in the kernel, so the kernel is a minimum. $\square$

Theorem 19 *Let $\mathcal{C} = \langle fh, 2fg \rangle$ be a quaternary cyclic code of odd length $n = p^2$ and $x^n - 1 = (x-1)ab$ where a and b are irreducible polynomials. Set $g = a$. If $f = b$ then $\mathcal{K}(\mathcal{C}) = \mathcal{C}$ and the kernel is a maximum. If $f = x - 1$ then $\mathcal{K}(\mathcal{C}) = \langle 2f \rangle$ and the kernel is a minimum.*

Proof: Let $\mathbf{v}$ be the vector corresponding to $fh = (x-1)b$. Then we have $2\mathbf{v} * \pi^j(\mathbf{v})$ is either $\mathbf{0}$, $2fh$ or a cyclic shift of the vector corresponding to $2b$. We note that $\mathbf{0}$ and $2fh$ are both in the code. So if $2b$ is in the code then the kernel is a maximum. If not then it is easy to see that no linear combination of the order 4 vectors is in the kernel and hence the kernel is a minimum.

If $f = b$, then $\mathcal{C} = \langle b(x-1), 2ba \rangle$. Then since $x-1$ and a are relatively prime, we have that $2b \in \langle 2b(x-1), 2ba \rangle$. Hence, in this case we have that $\mathcal{C} = \mathcal{K}(\mathcal{C})$.

If $f = x - 1$, then $\mathcal{C} = \langle (x-1)b, 2(x-1)a \rangle$. Then $2b \notin \langle (x-1)b, 2(x-1)a \rangle$ since $(x-1)$ does not divide b. Hence, in this case we have that $\mathcal{K}(\mathcal{C}) = \langle 2f \rangle$ and is a minimum. $\square$

Theorem 20 *Let $\mathcal{C} = \langle fh, 2fg \rangle$ be a quaternary cyclic code of odd length $n = p^2$ and $x^n - 1 = (x-1)ab$ where a and b are irreducible polynomials. Set $g = b$. If $f, h \neq 1$ then $\mathcal{K}(\mathcal{C}) = \langle 2f \rangle$ and the kernel is a minimum.*

Proof: Let $\mathbf{v}$ be the vector corresponding to fh. Then we have $2\mathbf{v} * \pi^j(\mathbf{v})$ is either $\mathbf{0}$ or a cyclic shift of the vector corresponding to $2b$. Moreover, we can see that any linear combination $\mathbf{w}$ of order 4 vectors has a vector $\mathbf{w}'$ such that $2\mathbf{w} * \mathbf{w}'$ is a cyclic shift of the vector corresponding to $2b$.

If $f = a$ then $\mathcal{C} = \langle a(x-1), 2ab\rangle$. If $f = x-1$ then $\mathcal{C} = \langle a(x-1), 2(x-1)b\rangle$. In both cases we have that $2b$ is not in the code, because neither a nor $(x-1)$ divides b. $\square$

In the following theorem, we will summarize all the cases when $n = p^2$ and $x^n - 1$ has three factors.

Theorem 21 *Let $\mathcal{C} = \langle fh, 2fg\rangle$ be a quaternary cyclic code of length $n = p^2$ and $x^n - 1 = (x-1)ab$ where a and b are irreducible polynomials. Then $\mathcal{K}(\mathcal{C})$ is either the minimum $\langle 2f\rangle$, the maximum $\mathcal{C}$ or $\langle 1 + x + x^2 + \ldots + x^{n-1}, 2f\rangle$. That is, we have that the dimension of $ker(\phi(\mathcal{C}))$ is either $\gamma + \delta, \gamma + 2\delta$ or $\gamma + \delta + 1$.*

Proof: Let $x^n - 1 = (x-1)ab$, where a and b are the irreducible polynomials defined before. We will check all the possibilities for f, g, h, $fgh = x^n - 1$ and we determine, in each case if the kernel is the maximum, dimension $\gamma + 2\delta$; the minimum, dimension $\gamma + \delta$ or it has dimension $\gamma + \delta + 1$.

- If $g = 1$ or $g = x - 1$, then $\mathcal{K}(\mathcal{C}) = \mathcal{C}$ and the kernel is a maximum by Corollary 1. For the remainder assume $g \neq 1, x - 1$.
- If $f = 1$ then we know that $\mathcal{K}(\mathcal{C}) = \mathcal{C}$ by Corollary 1.
- Set $f = a$. If $h = 1$, then we apply Theorem 17 and $\mathcal{K}(\mathcal{C}) = \langle 1 + x + x^2 + \ldots + x^{n-1}, 2fg\rangle$; that is, the dimension of the kernel is $\gamma + \delta + 1$. If $h = x - 1$, then $g = b$ and, by Theorem 20 the kernel is a minimum. If $h = b$ or $h = b(x - 1)$, then $g = 1$ or $x - 1$ and it has been determined before.
- Set $f = b$. If $h = 1$, then we apply Theorem 17 and $\mathcal{K}(\mathcal{C}) = \mathcal{C}$; that is, the kernel is a maximum. If $h = x - 1$, then $g = a$ and, by Theorem 20 the kernel is also a maximum. If $h = a$ or $h = a(x - 1)$, then $g = 1$ or $x - 1$ and it has been determined before.
- If $f = x - 1$ and $g = a$ or $g = b$, then by Theorems 19 and 20 the kernel is a minimum. If $g = ab$, then by Theorem 12, the kernel is also a minimum.
- Let $f = (x - 1)a$, or $f = (x - 1)b$ and $g \neq 1, x - 1$. Then by Theorem 18 the kernel is a maximum in the case $p = 2$ and it is a minimum otherwise.
- If $f = ab$, then necessarily $g = 1$ or $x - 1$ and of $f = x^n - 1$, then $g = 1$. In all the cases, the kernel has been determined before.

$\square$

In Table 1, we can completely determine all possible kernels from the last theorem when $n = p^2$ and there are only 3 irreducible factors of $x^n - 1$. A $*$ in the table indicates that it takes on all possible values. In this case there are 27 cyclic codes represented in the table. We consider $p > 2$.

f	g	h	Kernel dimension	Reference
1	$*$	$*$	$\gamma + 2\delta$	Corollary 1
$*$	1	$*$	$\gamma + 2\delta$	Corollary 1
$*$	$x-1$	$*$	$\gamma + 2\delta$	Corollary 1
a	$(x-1)b$	1	$\gamma + \delta + 1$	Theorem 17
a	b	$x-1$	$\gamma + \delta$	Theorem 20
b	$(x-1)a$	1	$\gamma + 2\delta$	Theorem 17
b	a	$x-1$	$\gamma + \delta$	Theorem 20
$(x-1)$	a	b	$\gamma + \delta$	Theorem 19
$(x-1)$	b	a	$\gamma + \delta$	Theorem 20
$(x-1)$	ab	1	$\gamma + \delta$	Theorem 12
$(x-1)a$	b	1	$\gamma + 2\delta$	Theorem 18
$(x-1)b$	a	1	$\gamma + 2\delta$	Theorem 18

Table 1: Kernel dimension of quaternary cyclic codes of length $n = p^2$.

4 Ranks of Cyclic Codes

In this section, we shall describe the quaternary code $\mathcal{R}(\mathcal{C})$ and its binary image which is $\langle \phi(\mathcal{C}) \rangle$. It is immediate that if $\mathcal{K}(\mathcal{C}) = \mathcal{C}$ then $\mathcal{R}(\mathcal{C}) = \mathcal{C}$ since $\langle \phi(\mathcal{C}) \rangle = \phi(\mathcal{C})$. We begin with a lemma.

Lemma 6 *Let $\mathcal{C}$ be a quaternary cyclic code. Then $\langle \phi(\mathcal{C}) \rangle$ is a quasi-cyclic code of index 2.*

Proof: Let $\{\mathbf{v}_i\}$ be a set of vectors in $C = \phi(\mathcal{C})$, then if $\mathbf{v} = \sum \alpha_i \mathbf{v}_i$ then $\sum \alpha_i \pi^2(\mathbf{v}_i) \in C$ and $\sum \alpha_i \pi^2(\mathbf{v}_i) = \pi^2(\mathbf{v})$. Hence the code is quasi-cyclic of index 2. $\square$

Note that we are not asserting that the binary image is linear, only that it is held invariant by the action of π^2.

Theorem 22 *Let $\mathcal{C}$ be a quaternary cyclic code, then $\mathcal{R}(\mathcal{C})$ is a quaternary cyclic code.*

Proof: By Lemma 1 we have that $\mathcal{R}(\mathcal{C})$ is linear. By Lemma 6 we have that $\langle \phi(\mathcal{C}) \rangle$ is quasi-cyclic of index 2, hence $\mathcal{R}(\mathcal{C})$ is a linear quaternary cyclic code. $\square$

In general, we have that $\mathcal{R}(\mathcal{C}) = \langle f'h', 2f'g' \rangle$ for some f', h', g' satisfying $f'g'h' = x^n - 1$.

The following lemma can be found in [11] and [10].

Lemma 7 *Let $\mathcal{C}$ be a quaternary code of type $4^\delta 2^\gamma$. Let $\{\mathbf{v}_1, \ldots, \mathbf{v}_\delta\}$ and $\{\mathbf{w}_1, \ldots, \mathbf{w}_\gamma\}$ be the sets of generators vectors of order 4 and 2 respectively. Then the quaternary code $\mathcal{C}' = \langle \mathcal{C}, \{2\mathbf{v}_i \star \mathbf{v}_j\}_{i,j \in \{1,\ldots,\delta\}} \rangle$ is the minimum quaternary linear code containig $\mathcal{C}$ such that $\phi(\mathcal{C}')$ is a binary linear code.*

Note that $\mathcal{C}$ has a binary linear image if and only if $2\mathbf{v}_i \star \mathbf{v}_j \in \mathcal{C}$ for any $i, j \in \{1, \ldots, \delta\}$. Since $\mathcal{R}(\mathcal{C})$ is, by definition, the minimum quaternary linear code containig $\mathcal{C}$ whose binary image is linear, then we can easily obtain the following corollary.

Corollary 7 *Let $\mathcal{C} = \langle fh, 2fg \rangle$ be a quaternary cyclic code of odd lenth. Then $\mathcal{R}(\mathcal{C}) = \langle \mathcal{C}, 2\mathbf{v} * \pi(\mathbf{v}), \ldots, 2\mathbf{v} * \pi^s(\mathbf{v}) \rangle$ where $\mathbf{v}$ is the vector corresponding to fh and $s = n - \deg(fh) - 1$.*

Theorem 23 *Let C be a quaternary cyclic code of odd length, with $C = \langle fh, 2fg \rangle$. Then there exits a polynomial r dividing f such that $\mathcal{R}(\mathcal{C}) = \langle fh, 2\frac{f}{r}g \rangle$.*

Proof: Let $\mathcal{C} = \langle fh, 2fg \rangle$ and $\mathcal{R}(\mathcal{C}) = \langle f'h', 2f'g' \rangle$. By Corollary 7, we have that $\mathcal{C}$ and $\mathcal{R}(\mathcal{C})$ have the same number of order 4 vectors. Since $\mathcal{C} \subseteq \mathcal{R}(\mathcal{C})$ we have that $fh = f'h'$. Then $fhg = f'h'g' = x^n - 1$ which gives that $g = g'$. Finally, we have that f' divides f by Theorem 3 and hence there exists a polynomial r such that $f'r = f$. Therefore, $\langle f'h', 2f'g' \rangle = \langle fh, 2\frac{f}{r}g \rangle$. □

We can use these results to find a maximum for $\mathcal{R}(\mathcal{C})$.

Theorem 24 *Let $\mathcal{C}$ be a quaternary cyclic code of odd length. If $\mathcal{C} = \langle fh, 2fg \rangle$ then $\mathcal{R}(\mathcal{C}) \subseteq \langle fh, 2g \rangle$ and $rank(\phi(\mathcal{C})) \leq \gamma + 2\delta + (\deg(f))$.*

Proof: Let $\mathcal{C} = \langle fh, 2fg \rangle$, and $\mathcal{R}(\mathcal{C}) = \langle fh, 2\frac{f}{r}g \rangle$ for some polynomial r. Then $\mathcal{R}(\mathcal{C}) \subseteq \mathcal{C}' = \langle f'h', 2f'g' \rangle$ where $f' = 1, h' = fh$ and $g = g'$. Note that $\mathcal{C}'$ has linear image by Corollary 1. Then

$$dim(\phi(\mathcal{C}')) = 4^{\deg(g')}2^{\deg(h')} = 4^{\deg(g)}2^{\deg(fh)} = 4^{\deg(g)}2^{\deg(h)}2^{\deg(f)}.$$

Hence, since $\mathcal{C}'$ is the maximum code that $\mathcal{R}(\mathcal{C})$ can be, we have that the dimension can go up at most by $\deg(f)$. □

In general, we have that

$$\langle fh, 2fg \rangle \subseteq \mathcal{R}(\mathcal{C}) \subseteq \langle fh, 2g \rangle. \tag{5}$$

Theorem 25 *Let $\mathcal{C}$ be a quaternary cyclic code of odd length with $\mathcal{C} = \langle fh, 2fg \rangle$. If $\phi(\mathcal{C})$ is not linear and f is irreducible then $\mathcal{R}(\mathcal{C}) = \langle f, 2g \rangle$.*

Proof: We know by Theorem 23, that $\mathcal{R}(\mathcal{C}) = \langle fh, 2\frac{f}{r}g \rangle$ for some r dividing f. But since f is irreducible, we have that $r = 1$ or $r = f$. If $r = f$ then the image is linear. Therefore, if $\phi(\mathcal{C})$ is not linear, $\mathcal{R}(\mathcal{C}) = \langle fh, 2g \rangle$. □

Notice that this theorem completely determines all possible cases when $n = p^2$ and $x^n - 1 = (x-1)(1 + x^2 + \ldots + x^{p-1})(1 + x^p + x^{2p} + \ldots + x^{(p-1)p})$ and all factors are irreducible, since the only cases where the image is not linear have f irreducible. Hence, we know the rank for every code in the Table 1.

Theorem 26 *Let $\mathcal{C} = \langle fh, 2fg \rangle$ be a quaternary cyclic code of odd length. Assume the polynomial $x^{n-1} + x^{n-2} + \ldots + x + 1$ is irreducible over $\mathbb{Z}_4$. If $g = x^{n-1} + x^{n-2} + \ldots + x + 1$, $f = x - 1$ and $h = 1$, then $\mathcal{R}(\mathcal{C}) = \langle x - 1, 2(1 + x + x^2 + \ldots + x^{n-1}) \rangle$.*

In all other cases, $\mathcal{R}(\mathcal{C}) = \mathcal{C}$.

Proof: By Corollary 6, we have that the only case when $\phi(\mathcal{C})$ is not linear is when $g = x^{n-1} + x^{n-2} + \ldots + x + 1$, $f = x - 1$ and $h = 1$. In this case, it is easy to see that $\mathcal{R}(\mathcal{C}) = \langle x - 1, 2(1 + x + \ldots + x^{n-1}) \rangle$. This code has a linear image by Corollary 6 and is formed by adding $2\mathbf{v} * \pi(\mathbf{v})$ where $\mathbf{v}$ is the vector corresponding to $x - 1$. □

5 Kernels and Ranks of Negacyclic Codes

We begin our study of negacyclic codes with a theorem that is similar to Theorem 4.

Theorem 27 *Let $\mathcal{C}$ be a negacyclic code over $\mathbb{Z}_4$. Then $\mathcal{K}(\mathcal{C})$ is a negacyclic code.*

Proof: The proof follows similarly to the proof of Theorem 4, replacing π with σ. $\square$

For odd n we have a bijective correspondence between cyclic codes and negacyclic codes using the following map:

$$\mu : \mathbb{Z}_4[x]/\langle x^n - 1\rangle \to \mathbb{Z}_4[x]/\langle x^n - 1\rangle, \tag{6}$$

where $\mu(c(x)) = c(-x)$.

Notice that from this bijective correspondence the role played by the all-one vector is now played by the vector $(1, 3, 1, 3, 1, 3, \ldots, 1)$. It is still true that if this vector is in the code, then $2(1, 3, 1, 3, 1, 3, \ldots, 1) * \mathbf{v} = 2\mathbf{v}$ and hence in the code. So that if this vector is in the code then this vector is in the kernel. The same can be said for any vector whose coordinates are all ± 1.

Theorem 28 *Let $\mathcal{C}$ be a cyclic code over $\mathbb{Z}_4$ then $\mu(\mathcal{K}(\mathcal{C})) = \mathcal{K}(\mu(\mathcal{C}))$.*

Proof: Assume $\mathbf{v} \in \mathcal{K}(\mathcal{C})$, then $2\mathbf{v} * \mathbf{w} \in \mathcal{C}$, for all $\mathbf{w} \in \mathcal{C}$. View $\mathbf{v}, \mathbf{w}$ as polynomials. Then $2\mathbf{v}(-x) * \mathbf{w}(-x) = 2\mathbf{v}(x) * \mathbf{w}(x)$ which is in $\mathcal{C}$. Note however that if $\mathbf{c} \in 2\mathbb{Z}_4^n$ then $\mu(\mathbf{c}) = \mathbf{c}$. Hence $2\mathbf{v} * \mathbf{w} \in \mu(C)$ and therefore $\mu(\mathbf{v}) \in \mathcal{K}(\mu(\mathcal{C}))$. Hence $\mu(\mathcal{K}(\mathcal{C})) \subseteq \mathcal{K}(\mu(\mathcal{C}))$.

Notice that $\mu(\mu(\mathbf{v})) = \mathbf{v}$. Let $\mu(\mathbf{v}) \in \mathcal{K}(\mu(\mathcal{C}))$. Then $2\mu(\mathbf{v}) * \mu(\mathbf{w}) \in \mu(\mathcal{C})$ for all $\mu(\mathbf{w}) \in \mu(\mathcal{C})$. Then by applying μ we have $2\mathbf{v} * \mathbf{w} \in \mathcal{C}$ for all $\mathbf{w} \in \mathcal{C}$. This gives the other direction. $\square$

We have similar theorems for the rank.

Theorem 29 *Let $\mathcal{C}$ be a quaternary cyclic code over $\mathbb{Z}_4$ then $\mu(\mathcal{R}(\mathcal{C})) = \mathcal{R}(\mu(\mathcal{C}))$.*

Proof: Consider the binary code $\phi(\mathcal{C})$ and the binary code $\phi(\mu(\mathcal{C}))$. The second binary code is formed from the first by simply permuting the two coordinates corresponding to odd powered monomials. Let this action be given by τ. Then $\tau(\phi(\mathcal{C})) = \phi(\mu(\mathcal{C}))$. It is immediate that $\tau(\langle\phi(\mathcal{C})\rangle) = \langle\phi(\mu(\mathcal{C}))\rangle$. Then by considering the inverse image under ϕ we have the result. $\square$

Theorem 30 *Let $\mathcal{C}$ be a quaternary negacyclic code then $\mathcal{R}(\mathcal{C})$ is a negacyclic code.*

Proof: If $\mathcal{C}$ is a quaternary negacyclic code then $\mathcal{C} = \mu(\mathcal{C}')$ for some quaternary cyclic code. Then by Theorem 29, $\mathcal{R}(\mathcal{C}) = \mu(\mathcal{R}(\mathcal{C}'))$. Since $\mathcal{C}'$ is cyclic, we have that $\mathcal{R}(\mathcal{C})$ is cyclic by Theorem 22. Then $\mu(\mathcal{R}(\mathcal{C}))$ is negacyclic and we have the result. $\square$

Given Theorem 28 and Theorem 29, we see that the case for negacyclic codes is determined by the case for cyclic codes.

6 Examples

We shall look at the rank and the kernel for some small values of n. For $n = 3, 5, 11, 13$, we have seen that the polynomial $x^{n-1} + x^{n-2} + \ldots + x + 1$ is irreducible, so these cases are trivial as described in Corollary 6 and Theorem 26.

In the cases $n = 7, 9, 17$, the polynomial $x^n - 1$ factors into three irreducible polynomials and the different values for the dimension of the kernel belong to $\{\gamma + \delta, \gamma + \delta + 1, \gamma + 2\delta\}$. We completely describe the case $n = 9$ at the Table 1. We add the results for the case $n = 7$ in the following tables. In the first table, the codes are linear; that is the dimension of the kernel is $\gamma + 2\delta$. In the second table the dimension of the kernel is the minimum possible; that is, $\gamma + \delta$. Finally, there are two cases where the dimension of the kernel is $\gamma + \delta + 1$.

$ker = \gamma + 2\delta$	γ, δ	ker
$f(x) = (x-1)(x^3+2x^2+x+3)(x^3+3x^2+2x+3);$ $g(x) = 1;$ $h(x) = 1.$	$7, 0$	7
$f(x) = (x-1)(x^3+2x^2+x+3);$ $g(x) = 1;$ $h(x) = (x^3+3x^2+2x+3).$	$3, 0$	3
$f(x) = (x-1);$ $g(x) = (x^3+2x^2+x+3);$ $h(x) = (x^3+3x^2+2x+3).$	$3, 3$	9
$f(x) = (x-1)(x^3+3x^2+2x+3);$ $g(x) = 1;$ $h(x) = (x^3+2x^2+x+3).$	$3, 0$	3
$f(x) = (x-1);$ $g(x) = (x^3+3x^2+2x+3);$ $h(x) = (x^3+2x^2+x+3).$	$3, 3$	9
$f(x) = (x-1);$ $g(x) = 1;$ $h(x) = (x^3+2x^2+x+3)(x^3+3x^2+2x+3).$	$6, 0$	6
$f(x) = (x^3+2x^2+x+3)(x^3+3x^2+2x+3);$ $g(x) = (x-1);$ $h(x) = 1.$	$0, 1$	2
$f(x) = (x^3+2x^2+x+3);$ $g(x) = (x-1);$ $h(x) = (x^3+3x^2+2x+3).$	$3, 1$	5
$f(x) = 1;$ $g(x) = (x-1)(x^3+2x^2+x+3)(x^3+3x^2+2x+3);$ $h(x) = 1.$	$0, 7$	14
$f(x) = 1;$ $g(x) = (x-1)(x^3+2x^2+x+3);$ $h(x) = (x^3+3x^2+2x+3).$	$3, 4$	11
$f(x) = (x^3+3x^2+2x+3);$ $g(x) = (x-1);$ $h(x) = (x^3+2x^2+x+3).$	$3, 1$	5
$f(x) = 1;$ $g(x) = (x-1)(x^3+3x^2+2x+3);$ $h(x) = (x^3+2x^2+x+3).$	$3, 4$	11
$f(x) = 1;$ $g(x) = (x-1);$ $h(x) = (x^3+2x^2+x+3)(x^3+3x^2+2x+3).$	$6, 1$	8
$f(x) = (x^3+2x^2+x+3)(x^3+3x^2+2x+3);$ $g(x) = 1;$ $h(x) = (x-1).$	$1, 0$	1
$f(x) = (x^3+2x^2+x+3);$ $g(x) = 1;$ $h(x) = (x-1)(x^3+3x^2+2x+3).$	$4, 0$	4

$f(x) = 1;$ $g(x) = (x^3 + 2x^2 + x + 3)(x^3 + 3x^2 + 2x + 3);$ $h(x) = (x - 1).$	$1, 6$	13
$f(x) = 1;$ $g(x) = (x^3 + 2x^2 + x + 3);$ $h(x) = (x - 1)(x^3 + 3x^2 + 2x + 3).$	$4, 3$	10
$f(x) = (x^3 + 3x^2 + 2x + 3);$ $g(x) = 1;$ $h(x) = (x - 1)(x^3 + 2x^2 + x + 3).$	$4, 0$	4
$f(x) = 1;$ $g(x) = (x^3 + 3x^2 + 2x + 3);$ $h(x) = (x - 1)(x^3 + 2x^2 + x + 3).$	$4, 3$	10
$f(x) = 1;$ $g(x) = 1;$ $h(x) = (x - 1)(x^3 + 2x^2 + x + 3)(x^3 + 3x^2 + 2x + 3).$	$7, 0$	7

$ker = \gamma + \delta$	γ, δ	ker
$f(x) = (x - 1)(x^3 + 2x^2 + x + 3);$ $g(x) = (x^3 + 3x^2 + 2x + 3);$ $h(x) = 1.$	$0, 3$	3
$f(x) = (x - 1)(x^3 + 3x^2 + 2x + 3);$ $g(x) = (x^3 + 2x^2 + x + 3);$ $h(x) = 1.$	$0, 3$	3
$f(x) = (x - 1);$ $g(x) = (x^3 + 2x^2 + x + 3)(x^3 + 3x^2 + 2x + 3);$ $h(x) = 1.$	$0, 6$	6
$f(x) = (x^3 + 2x^2 + x + 3);$ $g(x) = (x^3 + 3x^2 + 2x + 3);$ $h(x) = (x - 1).$	$1, 3$	4
$f(x) = (x^3 + 3x^2 + 2x + 3);$ $g(x) = (x^3 + 2x^2 + x + 3);$ $h(x) = (x - 1).$	$1, 3$	4

$ker = \gamma + \delta + 1$	γ, δ	ker
$f(x) = (x^3 + 2x^2 + x + 3);$ $g(x) = (x - 1)(x^3 + 3x^2 + 2x + 3);$ $h(x) = 1.$	$0, 4$	5
$f(x) = (x^3 + 3x^2 + 2x + 3);$ $g(x) = (x - 1)(x^3 + 2x^2 + x + 3);$ $h(x) = 1.$	$0, 4$	5

From Corollary 4, we know that the dimension of the kernel is $\gamma + \delta + \rho$, where ρ is the degree of a polynomial dividing g. Nevertheless, given the previous results and examples, one may think that for all cyclic codes of odd length, the dimension of the kernel is either the minimum, the maximum or the minimum plus 1, that is $\gamma + \delta$, $\gamma + 2\delta$ or $\gamma + \delta + 1$. This is true for all $n < 15$. For $n = 3, 5, 11, 13$ the polynomial $x^{n-1} + x^{n-2} + \ldots + x + 1$ is irreducible so we

can invoke Corollary 6. The cases for $n = 7$ and $n = 9$ are similar. However, at $n = 15$ there are codes for which this is not true. In the next example we shall show cases where the dimension of the kernel is neither the minimum, maximum, nor the minimum plus 1. But rather where it goes up by the degree of a factor of g.

Example 3 *Let $n = 15$. Here $x^{15} - 1 = (x-1)(x^2+x+1)(x^4+2x^2+3x+1)(x^4+3x^3+2x^2+1)(x^4+x^3+x^2+x+1)$. Hence there are $3^5 = 243$ cyclic codes of length 15. We shall give four examples where the dimension of the binary kernel is neither $\gamma+\delta, \gamma+\delta+1$, nor $\gamma+2\delta$.*

- *The first example is when $f = (x-1), g = (x^2+x+1)(x^4+2x^2+3x+1)(x^4+x^3+x^2+x+1)$ and $h = (x^4+3x^3+2x^2+1)$ then $\mathcal{C} = \langle fh, 2fg\rangle$ has $dim(ker(\phi(\mathcal{C}))) = \gamma+\delta+4 = 18$.*
- *The second example is when $f = (x-1), g = (x^2+x+1)(x^4+2x^2+3x+1)$ and $h = (x^4+3x^3+2x^2+1)(x^4+x^3+x^2+x+1)$ then $\mathcal{C} = \langle fh, 2fg\rangle$ has $dim(ker(\phi(\mathcal{C}))) = \gamma+\delta+4 = 18$.*
- *The third example is when $f = (x-1), g = (x^2+x+1)(x^4+3x^3+2x^2+1)(x^4+x^3+x^2+x+1)$ and $h = (x^4+2x^2+3x+1)$ then $\mathcal{C} = \langle fh, 2fg\rangle$ has $dim(ker(\phi(\mathcal{C}))) = \gamma+\delta+4 = 18$.*
- *The fourth example is when $f = (x-1), g = (x^2+x+1)(x^4+3x^3+2x^2+1)$ and $h = (x^4+2x^2+3x+1)(x^4+x^3+x^2+x+1)$ then $\mathcal{C} = \langle fh, 2fg\rangle$ has $dim(ker(\phi(\mathcal{C}))) = \gamma+\delta+4 = 18$.*

In all other cases for $n = 15$, we have that $dim(ker(\phi(\mathcal{C})) \in \{\gamma+\delta, \gamma+2\delta, \gamma+\delta+1\}$.

References

[1] T. Blackford, "Negacyclic duadic codes", Finite Fields Appl. Vol. 14, No. 4, 930 - 943, 2008.

[2] T. Blackford, "Cyclic codes over $\mathbb{Z}_4$ of oddly even length", International Workshop on Coding and Cryptography (WCC 2001) (Paris). Discrete Appl. Math. Vol. 128, No. 1, 27 - 46, 2003.

[3] T. Blackford, "Negacyclic codes over $\mathbb{Z}_4$ of even length", IEEE Trans. Inform. Theory, Vol. 49, No. 6, 1417 - 1424, 2003.

[4] J. Borges, C. Fernández and J. Rifà, "Propelinear structure of $\mathbb{Z}_{2k}$-linear codes", Technical Report arxiv:0907.5287, 2009.

[5] J. Borges, K.P. Phelps, J. Rifà, and V. Zinoviev, "On $\mathbb{Z}_4$-linear Preparata-like and Kerdock-like", IEEE Tans. Inf. Theory, Vol. 49, No.11, 2834 - 2843, 2003.

[6] A.R. Calderbank, N.J.A. Sloane, "Modular and p-adic cyclic codes", Des. Codes Cryptogr., Vol. 6, No. 1, 21 - 35, 1995.

[7] J.H. Conway and N.J.A. Sloane, "Self-dual codes over the integers modulo 4", J. Combin. Theory Ser. A , Vol. 62, 30 - 45, 1993.

[8] S.T. Dougherty, S. Ling, "Cyclic codes over $\mathbb{Z}_4$ of even length", Des. Codes Cryptogr., Vol. 39, No. 2, 127 - 153, 2006.

[9] C. Fernández-Córdoba, J. Pujol and M. Villanueva, "On rank and kernel of $\mathbb{Z}_4$-linear codes", Lecture Notes in Computer Science, No. 5228, 46 - 55, 2008.

[10] C. Fernández-Córdoba, J. Pujol and M. Villanueva, "$\mathbb{Z}_2\mathbb{Z}_4$-linear codes: rank and kernel", Des. Codes Cryptogr., Vol. 56, No. 1, 43 - 59, 2010.

[11] A.R. Hammons, P.V. Kumar, A.R. Calderbank, N.J.A. Sloane, P. Solé, "The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals and related codes", IEEE Trans. Inform. Theory., Vol. 40, No. 2, 301 - 319, 1994.

[12] V.S. Pless, P. Solé and Z. Qian, "Cyclic Self-Dual $\mathbb{Z}_4$-Codes", Finite Field and their applications, Vol. 3, No. 1, 48 - 69, 1997.

[13] V.S. Pless and Z. Qian, "Cyclic codes and quadratic residue codes over $\mathbb{Z}_4$", IEEE Trans. Inform. Theory., Vol. 42, No. 5, 1594 - 1600, 1996.

[14] J. Wolfmann, "Binary images of cyclic codes over $\mathbb{Z}_4$", IEEE Tans. Inf. Theory, Vol. 47, No 5, 1773 - 1779, 2001.